UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,572	12/03/2003	Ikuo Makita	1538.1043	5135

21171   7590   02/08/2008

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
GEE, JASON KAI YIN

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/725,572	MAKITA ET AL.
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03 December 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final. .

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims .

4)☒ Claim(s) <u>1-54</u> is/are pending in the application.

  4a) Of the above claim(s) <u>10-18,28-36 and 46-54</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-9,19-27 and 37-45</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All   b)☐ Some * c)☐ None of:

  1.☐ Certified copies of the priority documents have been received.

  2.☐ Certified copies of the priority documents have been received in Application No. _____.

  3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892) .

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) .

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>/06</u>.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is response to communication: amendment filed on 12/03/2007 with acknowledgement of benefit date of 06/27/2001.

2.   Claims 1-9, 19-27, and 37-45 are currently pending in this application. Claims 1, 7, 19, 25, 37, and 43 are independent claims.

3.   No new IDS has been received for this application.

Response to Arguments

4.   Applicant's arguments filed in regards to the some of the 112 rejections have been fully considered but they are not persuasive.

5.   As per the 112 rejections regarding claims 3, 21, and 39, the applicants argue that it is not unclear. The applicants bring in the specification to prove their point. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., that the format reverse-conversion program itself may have been originally stored in the intermediary computer, and sent to the first computer before receiving said digital signature) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Further, in independent claim 1, the receiving step only recites that first data and a first digital signature for the data is recieved. A format reverse-conversion program is never received in the receiving step. It is unclear why an additional digital signature would

need to be received when for a format reverse-conversion program is never received in

the first place.

In regards to the 112 rejections involving claims 6, 24, and 42, the applicants

recite that the second digital signature is recited in claim 2. However, these claims are

not dependent on claim 2, but claim 1, and thus, are still unclear.

6.   Applicant's arguments with respect to the other claims which have been

amended have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

8.   Claims 3-6, 21-24, 39-42 are rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as the invention.

As per claims 3-5, 21-23, 39-41 claims 3, 21, and 39 recite "wherein a third digital

signature for at least said format reverse-conversion program is received in said

receiving step." However, the receiving step never recites that a format reverse-

conversion program is ever received in the receiving step. It is unclear why a digital

signature needs is received for such a program.

As per claims 3-6, 21-24, 39-41, and 42, these claims recite a third digital

signature. It is unclear if there is a second digital signature involved, as only a first

digital signature is claimed in the claims in which they are dependent on.

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 1, 2, 7-9, 19, 20, 25-27, 37, 38, and 43-45 are rejected under 35

U.S.C. 103(a) as being unpatentable over Micali US patent No. 5,553,145 (hereinafter

Micali), and in view of Schneier's *Applied Cryptography*, 2nd Edition (hereinafter

Schneier).

As per claim 1, Micali teaches an information processing method executed by an

intermediary computer that can communicate with a first computer and a second

computer, said information processing method comprising: receiving first data and a first

digital signature for at least said first data from said first computer (col. 6 line 45 to col. 7

line 15 and col. 8 lines 35-44, wherein the first message is $E_{PO}(Sig_A(B, E_b(m)))$;

performing format conversion corresponding to a destination of said first data, for said

first data received in said receiving to generate second data (format conversion would

be hashing, as taught in col. 5 line 67 to col. 6 line 5); encrypting at least said second

data (as suggested in col. 8 lines 35-45, this would generate the message

$E_B(Sig_{PO}(Sig_A(B,E_b(m))))$ – which is equivalent to Alice's original message unencrypted

using Post office's public key, signed by Post office, and then encrypted by Post Office

using Bob's public key); sending at least the encrypted second data, a format reverse-

conversion program for performing reverse conversion of the format conversion, and

said first digital signature to said second computer associated with said destination.

(col. 6 lines 60 to col. 7 line 16 and col. 8 lines 15-45, wherein the format reverse-

conversion program is taught in col. 6 lines 63-68 "If this is the case, then it {Post Office}

sends to Bob information enabling him to retrieve Alice's message, preferbly using

digital signatures, and indicating to him but hiding from others that it is a piece of ICM

from Alice to him...", also, this is taught in col. 12 lines 25-35, where information is sent

to reconstruct the message; also, this section additionally teaches Bob receiving Alice's

signature.

To clarify this, Schneier's is combined with the reference for further details on the

method steps. As can be seen in the example on the bottom of page 40, Alice signs a

message. Trent verifies the signature. Trent signs the signed message (this would be

format conversion), and sends it to Bob. Bob verifies Trent's signature. In order for Bob

to verify Trent's signature, Bob would need some type of information from Trent. This

would probably be Trent's public key. This is seen in page 39 of Schneier, where

verifying a signature requires the public key of the signer. In addition, Schneier teaches

the use of one way hash functions. This is taught on pages 30 and 31. One-way hash

functiosn may utilize keys. The key would, in this case, be the format reversion program, as the format reversion would verify the hash value. As taught throughoutt Micali, the Post Office sends any additional information to Bob that it may need to reconstruct the message.

At the time of the invention, it would have been obvious to combine the Micali and Schneier references. One of ordinary skill in the art would have been motivated to perform such an addition to increase security. Micali already teaches the security aspects of the invention, and Schneier is used to supplement those teachings. Schneier is directed toward well known cryptographic methods, and it would have been obvious to incorporate the teachings of Schneier to clarify the aspects of cryptography that are well known in the art.

As per claim 2, Micali teaches further generating a second digital signature for at least said second data generated in said performing format conversion, said format reverse-conversion program, and said first digital signature, wherein said second digital signature is sent to said second computer in said sending step (col. 6 liens 60-67, col. 7 lines 1-10; col. 8 lines 35-45. The MIcali teaches throughout the reference that all the contents inside the message is digitally signed.

Claim 7 is rejected using the same basis of argument used to reject claim 1 above. Identification information is taught throughout Micali, such as in col. 6 lines 1-5, col. 6 lines 15-36, and throughout the reference.

Claim 8 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 9, is rejected using the same basis of arguments used to reject claim 8 above. Generating generating digital signatures by the intermediary is taught throughout Micali, as rejected above.

Independent claim 19 is rejected using the same basis of arguments used to reject claim 1 above.

Claim 20 is rejected using the same basis of arguments used to reject claim 2 above.

Claims 25-27 are rejected using the same basis of arguments used to reject claims 7-9 above.

Claim 37 is rejected using the same basis of arguments used to reject claim 1 above.

Claim 38 is rejected using the same basis of arguments used to reject claim 2 above.

Claims 43-45 are rejected using the same basis of arguments used to reject claims 25-27 above.

11. Claims 3, 4, 6, 21, 22, 24, 39, 40, and 42 are rejected under 35 U.S.C. 103(a) as being obvious over Micali and Schneier as applied above, and further in view of Menezes' *Handbook of Applied Cryptography* (1997) (hereinafter Menzes).

As per claim 3, as best understood by the Examiner, the Micali combination does not explicitly teach a third digital signature for at least said format reverse-conversion program in said receiving step. Micali already teaches the use of several digital signatures, which authenticate and prove to receivers that the senders/intermediaries are truly who they say they are. However, Micali does not explicitly teach sending digital signatures for each of the items sent. Micali teaches that the items sent are packaged, and sent with a digital signature. However, sending data individually and signing each message would have been obvious. Menezes teaches that digital signatures are used to bind identity to pieces of information. It would be obvious to bind every set of information with a signature, to increase security. This can be seen throughout Menezes, such as in pages 22 and 23. All the elements of a message may be signed, so that a receiver would be assured that each and every element is authentic. Again, this would provide assurance that each element is authenticated, and would increase security of the system.

As per claim 4, the claims recite generating a fourth digital signature for the package sent to the second computer (second data, format reverse-conversion program, third digital signature, first digital signature). As rejected in claim 3, Micali already teaches generating a digital signature at the intermediary for the package sent to the receiver. The other digital signatures (signatures for the items in each package), would have been obvious to perform to create more security.

As per claim 6, Namba teaches wherein said format reverse-conversion program and a third digital signature for said format reverse-conversion program are received in

said receiving step (col. 10 lines 16-50, where the intermediaries receive/retrieve the format reverse-conversion program; as seen in claim 3 above, a digital signature may encompass any part of a message, as it would increase security, as shown in Menezes).

Claims 21, 22, and 24, as best understood by the Examiner, are rejected using the same basis of arguments used to reject claims 3-6 above.

Claims 39, 40, and 42, as best understood by the Examiner, are rejected using the same basis of arguments used to reject claims 3-6 above.

12.   Claims 5, 23, and 41 are rejected under 35 U.S.C. 103(a) as being obvious over Micali and Schneier as applied above, and further in view of Namba US Patent No. 5,966,448 (hereinafter Namba)

As per claim 5, the Micali combination does not explicitly teach receiving a request for sending a format reverse-conversion program from said first computer, said request including designation of a destination. However, this is taught by Namba, such as in col. 11 line 60 to col. 12 line 50; col. 13 lines 30-63). Micali teaches the other limitations of this claim, such as in col. 7 lines 17 to col. 8 line 45.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the references of Namba and Micali. Both deal with communications utilizing a trusted intermediary. It is already taught by Micali that "it is preferable that these signatures are also forwarded to Bob" (col. 7 lines 5-10) By forwarding the

signatures of the original sender, the receiver will be assured that the messages truly come from the sender. Further, it is taught in Micali in col. 3 lines 50-55 that it would be beneficial where the recipient can prove the content of a message. Both the references are directed to secure messaging, and combining the references would create more security.

Claim 23 is rejected using the same basis of arguments used to reject claim 5 above.

Claim 41 is rejected using the same basis of arguments used to reject claim 5 and 23 above.

Conclusion

13.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of
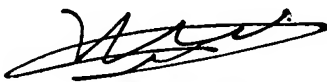
the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-38383811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2100
01/31/2008

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER